IN THE CLAIMS

PLEASE AMEND THE CLAIMS AS FOLLOWS:

1. (previously presented) A method for classifying a message, comprising:

extracting a plurality of reference points from a body of the message, each reference point being information used to contact a referenced entity;

classifying each of the plurality of reference points based on a source associated with each reference point;

determining whether the message is a fraudulent message appearing to be from a legitimate source based on the classified reference points; and

processing the message based on the determination of whether the message is a fraudulent message appearing to be from a legitimate source.

2. (previously presented) The method of claim 1, wherein classifying the plurality of reference points includes looking up the plurality of reference points in a database.

3. (previously presented) The method of claim 1, wherein detecting that the message is a fraudulent message appearing to be from a legitimate source includes determining that the message includes divergent reference points.

4. (previously presented) The method of claim 1, wherein detecting that the message is a fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a first source and a second reference point to a second source.

5. (previously presented) The method of claim 1, wherein detecting that the message is a fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a legitimate source and a second reference point to a questionable search.

6. (previously presented) The method of claim 1, wherein detecting that the message is a fraudulent message appearing to be from a legitimate source includes determining that the plurality of reference points includes a first reference point to a first source and a second reference point to a second source, and the second reference point is intended to appear as a reference to the first source.

7. (previously presented) The method of claim 1, further comprising computing a thumbprint of the message and storing the thumbprint to a database.

8. (previously presented) The method of claim 1, further comprising computing a thumbprint of the message and storing the thumbprint to a database; wherein the database is shared.

9. (previously presented) The method of claim 1, further comprising identifying a plurality of fraud indicators and applying a statistical analysis on the plurality of fraud indicators.

10. (previously presented) The method of claim 1, further comprising quarantining the message.

11. (previously presented) The method of claim 1, further comprising deleting the message.

12. (previously presented) The method of claim 1, further comprising providing an alert to a recipient of the message.

13. (previously presented) The method of claim 1, further comprising providing an alert to a recipient indicating that the message is a fraudulent message appearing to be from a legitimate source.

14. (previously presented) The method of claim 1, further comprising providing an explanation of the fraudulent message appearing to be from a legitimate source to a recipient.

15. – 25. (cancelled)

26. (previously presented) A computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for classifying a message, the method comprising:

extracting a plurality of reference points from a body of the message;

classifying the plurality of reference points;

determining whether the message is a fraudulent message appearing to be from a legitimate source based on the classified reference points; and

processing the message based on the determination of whether the message is a fraudulent message appearing to be from a legitimate source.

27. - 28. (cancelled)